SYSTEMS AND METHODS FOR COMPUTER DEVICE AUTHENTICATION

ABSTRACT

Systems and methods for device authentication using a master key that is stored in protected non-volatile memory. The master key is used to derive sensitive data that is transferred to storage that is only accessible in a privileged mode of operation of the computing system. The sensitive data and the master key are not directly accessible by programs that are not running in the privileged mode of operation. The master key is used to derive one or more application keys that are used to secure data that is specific to an application/device pair. Non-privileged programs can request functions that run in the privileged mode to use these application keys. The privileged mode program checks the integrity of the non-privileged calling program to insure that it has the authority and/or integrity to perform each requested operation. One or more device authority servers are used to issue and manage both master and application keys.